

**IN THE SUPERIOR COURT OF THE DISTRICT OF COLUMBIA**  
**Civil Division**

**DISTRICT OF COLUMBIA**

a municipal corporation  
441 4th Street, N.W.  
Washington, D.C. 20001,

Plaintiff,

v.

**FACEBOOK, INC.**

1 Hacker Way  
Menlo Park, CA 94025

*Serve on:*

**CORPORATION SERVICE CO.,**

**Registered Agent**

1090 Vermont Ave. N.W.  
Washington, D.C. 20005,

Defendant.

Case No.:

**COMPLAINT FOR VIOLATIONS OF THE CONSUMER PROTECTION**  
**PROCEDURES ACT**

Plaintiff District of Columbia (District), by the Office of the Attorney General, brings this action against Defendant Facebook, Inc. (Facebook) for violations of the District's Consumer Protection Procedures Act (CPPA), D.C. Code §§ 28-3901, *et seq.* In support of its claims, the District states as follows:

**Introduction**

1. This case stems from the failure by Defendant Facebook to honor its promise to protect its consumers' personal data. Facebook operates a website (www.facebook.com) and a companion mobile application through which it offers social networking services to its two billion active users, which includes hundreds of thousands of consumers in Washington, D.C.

(D.C.). Facebook collects and maintains a trove of its consumers' personal data, as well as data regarding consumers' digital behavior on and off the Facebook website. Facebook permits third-party developers—including developers of applications and mobile device makers—to access this sensitive information in connection with offering applications to Facebook consumers. Facebook's consumers reasonably expect that Facebook will take appropriate steps to maintain and protect their data. Facebook tells them as much, promising that it requires applications to respect a Facebook consumer's privacy. Facebook has failed to live up to this commitment.

2. These failures are highlighted through Facebook's lax oversight and enforcement of third-party applications. To provide just one example, from 2013-2015, Facebook permitted a Cambridge University researcher named Aleksandr Kogan (Kogan) to use a third-party application to harvest the personal data of approximately 70 million Facebook consumers in the United States and then sell it to Cambridge Analytica, a political consulting firm that relied on Facebook data to target voters and influence elections in the United States. Although Kogan's application was only installed by 852 distinct Facebook consumers in D.C., the application also collected the personal information of users' Facebook friends—including more than 340,000 of D.C.'s residents who did not download the application. This sequence of events was replete with failures in oversight and enforcement. For instance, as remains its policy to this day, Facebook failed to take the basic step of reviewing the terms of Kogan's application, which would have alerted the company to the fact that Kogan planned to improperly sell consumer data. Furthermore, after discovering the improper sale of consumer data by Kogan to Cambridge Analytica, Facebook failed to take reasonable steps to protect its consumers' privacy by ensuring that the data was accounted for and deleted. Facebook further failed to timely inform the public (including D.C. residents) that tens of millions of its consumers had their data sold to Cambridge

Analytica, even though Facebook knew, or should have known, that such data was acquired in violation of its policies and was being used in connection with political advertising.

3. These failures are also demonstrated by Facebook's relationship with partner companies, including mobile device makers. Facebook permitted select partner companies special access to its consumers' data in connection with the development of Facebook-related applications. Through these relationships, select partner companies were allowed to override Facebook consumers' privacy settings and access their information without their knowledge or consent.

4. Facebook's policies and practices relating to third party access and use of consumer data violate the District's consumer protection laws. First, Facebook misrepresented the extent to which it protects its consumers' personal data, requires third-party developers to respect its consumers' personal data, and how consumers' agreements with third-party applications control how those applications use their data. Second, Facebook failed to adequately disclose to Facebook consumers that their data can be accessed without their knowledge or affirmative consent by third-party applications downloaded by their Facebook friends. Third, Facebook failed to disclose to affected consumers when their data was improperly harvested and used by third-party applications and others in violation of Facebook's policies, such as in the Kogan and Cambridge Analytica example. Fourth, compounding these misrepresentations and disclosure failures, Facebook's privacy settings are ambiguous, confusing, and difficult to understand. Finally, Facebook failed to disclose that it granted certain companies, many of whom were mobile device makers, special permissions that enabled those companies to access consumer data and override consumer privacy settings.

5. Facebook could have prevented third parties from misusing its consumers' data had it implemented and maintained reasonable oversight of third-party applications consistent with its representations in its public statements, terms of service, and policies. The District brings this case to ensure that Facebook is held accountable for its failure to protect the privacy of its consumers' personal data. The District seeks injunctive relief to prevent Facebook from engaging in these and similar unlawful trade practices, civil penalties and costs to deter Facebook from engaging in these and similar unlawful trade practices, and any appropriate restitution for consumers.

### **Jurisdiction**

6. This Court has jurisdiction over the subject matter of this case pursuant to D.C. Code §§ 11-921 and 28-3909.

7. This Court has personal jurisdiction over Defendant Facebook pursuant to D.C. Code § 13-423(a).

### **Parties**

8. Plaintiff District of Columbia (District) is a municipal corporation empowered to sue and be sued, and is the local government for the territory constituting the permanent seat of the federal government. The District brings this case through the Attorney General for the District of Columbia, who is the chief legal officer for the District. The Attorney General is responsible for upholding the public interest and is also specifically authorized to enforce the District's consumer protection laws, including the CPPA.

9. Defendant Facebook, Inc. (Facebook), is a Delaware corporation with its headquarters and principal place of business at 1 Hacker Way, Menlo Park, CA, 94025.

Facebook engages in the business of supplying social networking services through the operation of its website, [www.facebook.com](http://www.facebook.com), and accompanying mobile applications, to consumers in D.C.

### **Facebook's Collection of Consumer Data**

10. The Facebook website<sup>1</sup> allows consumers to build a social network with other Facebook consumers and share information within that network. It is among the world's most heavily trafficked websites and has over two billion active consumers around the globe. Hundreds of thousands of D.C. residents are among Facebook's consumers.

11. To begin using the Facebook website, a consumer first creates a Facebook account. The consumer can then add other Facebook consumers as "friends" and by accumulating Facebook friends, the consumer builds a social network on the Facebook website.

12. As Facebook consumers grow their social networks and interact with friends on the Facebook website, their information and activity is digitally collected, recorded, and maintained by Facebook. As relevant here, this data can be divided into two broad categories: (i) data directly supplied by consumers, and (ii) data pertaining to consumers' activity on and off the Facebook website.

13. First, consumers directly provide Facebook with personal information. To create a Facebook account, a consumer is required to supply Facebook with basic information such as their name, phone number, email address, birthday, and gender. A consumer then has the option to customize their "Facebook Profile" by supplying additional information to Facebook, such as their hometown, educational history, work experience, relationship status, political and religious

---

<sup>1</sup> In this Complaint, the "Facebook website" refers to both (i) [www.facebook.com](http://www.facebook.com), which is accessed through an Internet browser, and (ii) the Facebook mobile application, which is accessed through a mobile device like a smartphone or tablet. Many of Facebook's features and services available on [www.facebook.com](http://www.facebook.com) are also available through the Facebook mobile application.

views, and personal photographs. Facebook's website is designed to encourage consumers to continue supplying information in the form of "Posts," which are shared with that consumer's friends. Posts include, but are not limited to, written statements, photographs and videos, links to websites, and "Check Ins" to geographic locations such as restaurants and bars.

14. Second, Facebook tracks and maintains data pertaining to consumer activity on its website. For example, Facebook records what advertisements are displayed to each consumer, as well as whether the consumer clicked on the advertisement. Facebook also tracks the date and time each consumer logs into their account, as well as the IP address, device, and browser they used to log in. Facebook also operates a companion mobile application called "Facebook Messenger," which allows Facebook consumers to send and receive messages and make phone and video calls. For users of Facebook Messenger, Facebook maintains records of messages sent and received and the date and time of phone and video calls made.

15. Another example of consumer activity data that Facebook collects is a consumer's "Likes," one of Facebook's signature innovations. It allows consumers to click on a "thumbs-up" icon to Like a vast array of online content. Among other things, Facebook consumers can Like "Posts" made by other Facebook consumers, "Pages" maintained by non-individual entities, and content on external websites.

16. Facebook's Like feature incentivizes increased activity on the Facebook website by allowing consumers to reward one another for sharing information—the more Posts a consumer makes, the more Likes they will receive. The Like also serves a broader function because over time, a consumer's allocation of Likes reveals information about them—the friends they interact with most, the brands that catch their eye, the issues with which they identify. Facebook records and maintains each and every one of its consumers' Likes.

17. Facebook generates much of its revenue by selling advertising space. Facebook relies on its collection of consumer data—and the personal information and preferences derived from each individual’s data—to sell targeted advertising space to marketers. Facebook’s business model primarily relies on using consumer data to provide advertisers the ability to run targeted ads to particular individuals and demographics. In other words, although Facebook supplies its social networking services free of direct monetary charge to consumers, in exchange, consumers provide Facebook with their personal data, which Facebook monetizes through the sale of targeted advertising.

#### **The Facebook Platform and Third-Party Facebook Applications**

18. In 2007, Facebook launched the Facebook Platform, an extensive software environment where third-party developers can build applications that interact with the Facebook website. The Facebook Platform includes various services and tools designed to assist third-party developers to create such applications.

19. Millions of third-party applications have been developed using the Facebook Platform and made available to Facebook consumers. Some applications are social, such as those that allow consumers to play games against other consumers within their social networks. Others are functional, allowing consumers to integrate information from their calendar and email accounts with their Facebook account.

20. The Facebook Platform facilitates integration between the Facebook website and third-party applications. For example, a third-party developer can allow Facebook consumers to access their application with a service available on the Facebook Platform called “Facebook Login.” Facebook Login allows a Facebook consumer to access an application directly by using

their Facebook account and login credentials (username and password). The Facebook Platform also harmonizes third-party applications' look and feel with the Facebook website.

21. The Facebook Platform also includes an application program interface (API). An API specifies how software components interact. In practical terms, Facebook's website is built upon proprietary source code. The API refers to the code that Facebook makes available to third-party developers, which enables those developers to build applications for the Facebook website. Facebook's API allows for a third-party application to interact with the Facebook website and governs the extent to which it can access Facebook's vast collection of consumer data.

22. In sum, the Facebook Platform was designed to allow for the development of third-party applications that would seamlessly engage with Facebook consumers while at the same time allowing those applications access to Facebook's vast collection of consumer data.

### **The Cambridge Analytica Data Harvest**

#### **A. The Harvest of 70 Million Facebook Consumers' Data**

23. In November 2013, Aleksandr Kogan, a researcher affiliated with Cambridge University, and his company, Global Science Research (GSR), launched a third-party application on the Facebook Platform that identified itself as a personality study for research purposes. The application was called "thisisyourdigitallife" (the App) and ran on the Facebook Platform for over two years. The App appealed to Facebook consumers as a personality quiz and offered to generate a personality profile for consumers in exchange for downloading the App and granting access to some of the consumer's Facebook data.

24. The App was presented to Facebook as a research tool to study psychological traits. At the time of the App's launch, third-party applications could be launched on the



Facebook Platform without affirmative review or approval by Facebook. Accordingly, Facebook did not review the App before it was allowed on the Facebook Platform, nor did it verify its claim that the information it collected was for academic purposes.

25. At the time of the App's launch, Facebook permitted applications to request permission to access a Facebook consumer's personal data. Prior to installation, a Facebook consumer installing the App (an App User) was shown a screen that stated that the App would download some of the App User's own Facebook data, including their name, gender, birthdate, Likes, and a list of Facebook friends.

26. To complete the installation, an App User clicked a Facebook Login icon on the information screen. The App was then installed through the Facebook Login service, using the App User's Facebook login credentials.

27. Upon installation, the App harvested the personal information of the App User from the Facebook collection of user data, including at least the App User's name, gender, birthday, Likes, and list of Facebook friends.

28. In addition, the App also accessed data of the App User's Facebook friends that the friend had shared with the App User. This data included at least the Facebook friend's name, gender, birthdate, current city, and Likes. The vast majority of these Facebook friends never installed the App, never affirmatively consented to supplying the App with their data, and never knew the App had collected their data.

29. In early 2014, Facebook introduced changes to the Facebook Platform that (i) limited the data that applications could access, including data regarding the installing user's friends, and (ii) instituted a review and approval process (App Review) for applications that sought to access data beyond what the updated Facebook Platform would allow. In May 2014,

Kogan applied to App Review to request access to consumer data beyond what the updated Facebook Platform would allow. In only a matter of days, Facebook rejected Kogan's application on the basis that he was seeking information beyond the App's stated research purposes. Nevertheless, the App was still permitted to access consumer data beyond what the updated Facebook Platform allowed through at least May 2015, due to a grace period Facebook granted existing applications following its update to the Facebook Platform. This grace period was not absolute, and Facebook made numerous exceptions for other applications.

30. During the time that the App ran on the Facebook Platform, approximately 290,000 Facebook consumers in the United States installed the App, including 852 consumers in D.C. Because the App was improperly allowed to harvest the personal data of App Users as well as App Users' Facebook friends, approximately 70 million United States Facebook consumers had their information collected by the App, including over 340,000 of D.C.'s residents.

B. The Sale and Misuse of Consumer Data

31. In 2014, at a time when the App was fully operational on the Facebook Platform and harvesting consumer data, Kogan entered into an agreement with Cambridge Analytica for the sale of data collected by the App. Cambridge Analytica was a political consulting firm based in London, England that provided consulting services to candidates running for political office in the United States and abroad.

32. Kogan provided Cambridge Analytica with the personal data and derivative data of the approximately 70 million United States Facebook consumers whose data was harvested, which included almost half of all D.C. residents. In exchange, Cambridge Analytica paid Kogan over \$800,000.

33. Cambridge Analytica used the data it acquired from Kogan to, among other things, target digital political advertising during the 2016 United States Presidential Election (the 2016 Election). Cambridge Analytica received millions of dollars from multiple presidential candidate campaigns to provide digital advertising services during the 2016 Election.

34. At relevant times, Facebook had employees embedded within multiple presidential candidate campaigns who worked alongside employees from Cambridge Analytica. Facebook knew, or should have known, that these presidential candidate campaigns and Cambridge Analytica were using the Facebook consumer data harvested by Kogan throughout the 2016 Election.

#### **Facebook's Lack of Oversight and Enforcement of Its Own Policies**

35. By no later than December 11, 2015, Facebook knew that Kogan had sold Facebook consumer data to Cambridge Analytica. At that time, Facebook also knew that the collection and sale of consumer data violated its Platform Policy.

36. Facebook's Platform Policy, which governed its relationship with third-party application developers throughout the App's operation on the Facebook Platform, expressly prohibited the transfer and sale of consumer data accessed from Facebook. However, Facebook failed to exert meaningful review or compliance mechanisms to enforce its Platform Policy. Indeed, the App itself contained terms that directly contradicted the Platform Policy, expressly stating that collected data could be used for commercial purposes. Nevertheless, Facebook did not take any action against the App and instead permitted it to harvest and sell Facebook consumers' data without oversight.

37. The Platform Policy also permitted Facebook to audit any applications on the Facebook Platform and to take other enforcement measures if it suspected that an application was violating the Platform Policy. In addition, the Platform Policy expressly provided several

methods by which Facebook could enforce non-compliance with the Platform Policy. These audit provisions were largely unenforced.

38. In late December 2015, Facebook terminated the App's access to the Facebook Platform. Nevertheless, Facebook did not ban, suspend, or limit the privileges of Kogan, Cambridge Analytica, or any of their affiliates, with respect to their access to the Facebook website or the Facebook Platform. Nor did Facebook conduct an audit of Kogan, Cambridge Analytica, or any of their affiliates, or take any other enforcement or remedial action to determine whether the Facebook consumer data that was harvested by the App had been accounted for, deleted, and protected from further use and sharing.

39. Instead, Facebook simply requested that Kogan and Cambridge Analytica delete all data that they received through the Facebook Platform, and accepted their word that they had done so. Facebook did not take any additional steps to determine whether the harvested data was, in fact, accounted for and destroyed. And in fact, the data was not destroyed. It continued to be held and used by Cambridge Analytica through the 2016 Election and beyond. Facebook knew, or should have known, this fact from, among other sources, its employees embedded in presidential candidate campaigns during the 2016 Election who worked alongside Cambridge Analytica employees.

40. Facebook eventually required written certifications promising that the harvested data was accounted for and destroyed, but Facebook did not receive a certification from Kogan until June 2016 and did not receive a certification from Cambridge Analytica until April 2017.

41. Years after their data was improperly harvested, in April 2018, Facebook finally disclosed to its consumers that their personal information may have been harvested and sold to Cambridge Analytica.

42. Had Facebook disclosed in 2015 or 2016 the sale of Facebook consumer data to Cambridge Analytica, it would have provided consumers with timely material information about their use of the Facebook website. A disclosure that Facebook consumers' data had been sold to a political consulting firm and was being used to target political advertising for the 2016 Election would have influenced Facebook consumers, including consumers in D.C. to, among other things, share less information on the Facebook website or deactivate their Facebook accounts. Rather than make such meaningful disclosures, Facebook instead profited from Kogan's and Cambridge Analytica's misuse of this stolen consumer data by selling millions of dollars of advertising space to Cambridge Analytica and presidential candidate campaigns during the 2016 Election.

43. Facebook knew of other third-party applications that similarly violated its Platform Policy through selling or improperly using consumer data. Facebook also failed to take reasonable measures to enforce its Platform Policy in connection with other third-party applications and failed to disclose to users when their data was sold or otherwise used in a manner inconsistent with Facebook's policies.

**Facebook's Misleading Statements and Practices Regarding Third-Party Application Access to Consumer Data**

44. Facebook made some disclosures about third-party application access to consumer data, but these disclosures were ambiguous, misleading, and deceptive. These disclosures primarily are contained in two lengthy documents, a Terms of Service and Data Policy, that consumers must agree to in order to create a Facebook account. These documents together set out the general terms of use for the Facebook website, and contain some statements regarding how third-party applications could access a consumer's data. However, as shown by Facebook's actions (and inactions) in connection with third parties, including the App and

Cambridge Analytica, the representations made in these documents were misleading and deceptive.

45. For the duration of the App's launch and operation on the Facebook Platform, Facebook's Terms of Service represented that Facebook required applications to respect a Facebook consumer's privacy. This representation, taken with Facebook's public statements that it would protect consumers' private information and its representations in the Platform Policy that it had the ability to audit applications and take enforcement measures against applications, gave consumers the impression that Facebook had implemented and maintained reasonable oversight and safeguards to protect consumers' privacy.

46. These representations were misleading and deceptive, as demonstrated by Facebook's lack of oversight and enforcement relating to third parties, such as the App. For example, Facebook failed to conduct meaningful oversight or enforcement of the App at several relevant times when it knew, or should have known, that the App was operating in violation of Facebook's policies: (i) when the App was first launched on the Facebook Platform; (ii) after Facebook became aware, through its receipt and rejection of Kogan's application through App Review, that the App was seeking consumer data to be used beyond the App's stated research purpose; and (iii) after it learned that data collected by the App had been sold to Cambridge Analytica.

47. In addition, Facebook's Data Policy also contained misrepresentations about third-party applications' access to Facebook consumer data. From at least November 15, 2013 to at least January 30, 2015, the Data Policy provided that if an application asks permission from someone else to access your information, the application will be allowed to use that information only in connection with the person that gave the permission, and no one else. This representation

was deceptive and misleading as demonstrated by Kogan's use of the App to harvest consumer data, and then sell it to Cambridge Analytica. Facebook failed to implement and maintain reasonable oversight of applications operating on the Facebook Platform to safeguard consumers' private data, and it knew or should have known that it did not have measures in place to control how applications used and/or shared data.

48. Facebook also misled its consumers generally about third-party applications' access to their data. Facebook publicly represented that consumers controlled how their data is shared on the Facebook website. But as shown by the App, third-party applications that a Facebook consumer had never downloaded could still access their information through a Facebook friend who downloaded the App. The Facebook Platform thus afforded third parties an end-run to access consumer data, which third-party applications exploited. This was a material fact that Facebook failed to disclose, or failed to adequately disclose, to its consumers.

49. Adding to the potential customer confusion is the fact that consumers could not restrict third-party application access to their data through Facebook's Privacy Settings, even though that is where a consumer would expect to have the ability to control how their data is shared. Instead, Facebook allocated privacy settings related to applications to a separate location under a separate Application Settings tab.

50. Through Privacy Settings, a consumer controls how their Facebook information is shared with other Facebook consumers. For example, a consumer can control what kinds of other Facebook users can view their account information. This can be manipulated to allow for sharing to all Facebook consumers (most expansive), only Facebook friends (the less expansive default), and a customized list of Facebook friends (the least expansive).

51. By contrast, through Application Settings, a consumer controls how their Facebook information is shared with third-party applications. There is a high potential for consumer confusion here. For example, from at least November 2013 through at least April 2014, even if a consumer restricted access to their information to only Facebook friends through their Privacy Settings, the information could still be accessible by any application that the consumer's friends downloaded.

52. In sum, Facebook's representations regarding consumer privacy in connection with applications were misleading and deceptive. Moreover, Facebook's lack of adequate disclosures and multi-tiered privacy options added to consumer confusion regarding how consumer information was shared with applications.

53. Facebook's representations to consumers that it will protect the privacy of consumers' personal information, when, in fact, it did not implement or maintain reasonable privacy safeguards and failed to take reasonable measures in response to the harvesting and use of data by Cambridge Analytica, are misrepresentations of material facts that tend to mislead consumers.

54. Facebook's representations to consumers that it requires applications and third-party developers to respect the privacy of consumers' personal information, when, in fact, it did not implement or maintain reasonable oversight of third-party applications (such as conduct appropriate audits of applications), are misrepresentations of material facts that tend to mislead consumers.

55. Facebook's representations to consumers that consumers' agreements with third-party applications will control how those applications use consumer data, when, in fact,



applications were able to collect and use consumer data without regard to those agreements, are misrepresentations of material facts that tend to mislead consumers.

56. Facebook's failure to inform consumers, or to adequately inform consumers, that their personal information may be shared with third-party applications without their knowledge or affirmative consent, is a material fact, the omission of which tended to mislead consumers.

57. Facebook's failure to tell consumers for over two years that their personal information was improperly harvested and sold by Kogan to Cambridge Analytica in violation of Facebook's policies is a material fact, the omission of which tended to mislead consumers.

58. Facebook's failure to explain to consumers how to control how information is shared with third-party applications and how to change privacy settings with respect to applications, and its representations that consumers can control how their information is shared, constitute ambiguities as to material facts that have the tendency to mislead consumers.

**Facebook's Misleading Statements and Practices Regarding Partner Company Access to Consumer Data**

59. In addition to third-party applications, Facebook also improperly granted certain partner companies, many of whom were mobile device makers, access to Facebook's collection of consumer data.

60. Today, most consumers accessing Facebook through their mobile devices do so through the Facebook mobile application developed for the leading smartphone operating systems. Prior to the widespread usage of the Facebook mobile application, however, Facebook entered into integration partnerships with various device makers to develop Facebook applications specific to their device.

61. For example, BlackBerry developed an application for BlackBerry devices called the "Hub," which was designed to allow BlackBerry users to view all their social media accounts

(including Facebook accounts) in one place. In order to build applications like the Hub, Facebook licensed to device makers limited rights to use APIs to create specific integrations between the device and Facebook, which were approved by Facebook.

62. Through these arrangements, applications like the Hub were permitted access to Facebook consumer data, including the data of the Facebook consumer who downloaded the application and the data of those consumers' Facebook friends. Consumers had little or no control over whether to permit the sharing of their information to these companies. For instance, even if a consumer denied Facebook permission to share their information with any third parties, applications like the Hub were able to override those sharing restrictions and access their data.

63. Facebook entered into at least 52 integration partnerships with other companies. Facebook also extended similar access to Facebook consumer data to other partner companies.

64. Facebook's failure to inform consumers that it permitted certain companies to override a Facebook consumer's privacy settings and access their information without their knowledge or consent constitute omissions of material facts that have the tendency to mislead consumers.

65. Facebook's representations that consumers can control how their information is shared, when, in fact, certain partner companies were able to override those controls, constitute misrepresentations as to material facts that have the tendency to mislead consumers.

**Count I: Violations of the Consumer Protection Procedures Act**

66. The District incorporates the allegations of paragraphs 1 through 65 into this Count.

67. The CPPA is a remedial statute that is to be broadly construed. It establishes an enforceable right to truthful information from merchants about consumer goods and services that are or would be purchased, leased, or received in the District of Columbia.

68. The services that Facebook provides consumers are for personal, household, or family purposes and, therefore, are consumer goods and services.

69. Facebook, in the ordinary course of business, supplies consumer goods and services and, therefore, is a merchant under the CPPA.

70. Facebook users receive consumer goods and services from Facebook in the form of social networking services and, therefore, are consumers under the CPPA.

71. The CPPA prohibits unfair and deceptive trade practices in connection with the offer, sale, and supply of consumer goods and services.

72. Facebook's representations to consumers, both express and implied, that it will protect the privacy of consumers' personal information, that it requires applications and third-party developers to respect the privacy of consumers' personal information, and that consumers' agreement with third-party applications will control how those applications use consumer data, are misrepresentations concerning material facts that have a tendency to mislead consumers and are unfair and deceptive trade practices that violate the CPPA, D.C. Code § 28-3904(e).

73. Facebook's failure to disclose, or failure to adequately disclose, to consumers that their personal information may be shared with third-party applications without their knowledge or affirmative consent, is a material fact, the omission of which tended to mislead consumers and are unfair and deceptive trade practices that violate the CPPA, D.C. Code § 28-3904(f).

74. Facebook's failure to disclose, or failure to adequately disclose, to consumers that their personal information was improperly harvested and used by third-party applications and

others in violation of Facebook's policies, such as in the Kogan and Cambridge Analytica example, is a material fact, the omission of which tended to mislead consumers and are unfair and deceptive trade practices that violate the CPPA, D.C. Code § 28-3904(f).

75. Facebook's failure to explain to consumers how to control how information is shared with third-party applications and how to change privacy settings with respect to applications, as well as its representations to consumers, both express and implied, that it will protect the privacy of consumers' personal information, that it requires applications and third-party developers to respect the privacy of consumers' personal information, and that consumers' agreement with third-party applications will control how those applications use consumer data, constitute ambiguities as to material facts that have the tendency to mislead consumers and are unfair and deceptive trade practices that violate the CPPA, D.C. Code § 28-3904(f-1).

76. Facebook's failure to disclose to consumers that it permitted certain companies to override a Facebook consumer's privacy settings and access their information without their knowledge or consent are material facts, the omission of which tended to mislead consumers and are unfair and deceptive trade practices that violate the CPPA, D.C. Code § 28-3904(f).

#### **Prayer for Relief**

WHEREFORE, the District of Columbia respectfully requests this Court enter a judgment in its favor and grant relief against Defendant Facebook, Inc. as follows:

- (a) Permanently enjoin Defendant, pursuant to D.C. Code § 28-3909(a), from violating the CPPA;
- (b) Order Defendant to pay restitution or damages pursuant to D.C. Code § 28-3909;
- (c) Award civil penalties in an amount to be proven at trial and as authorized per violation of the CPPA pursuant to D.C. Code § 28-3909(b);

(d) Award the District the costs of this action and reasonable attorney's fees pursuant to D.C. Code § 28-3909(b); and grant such further relief as the Court deems just and proper.

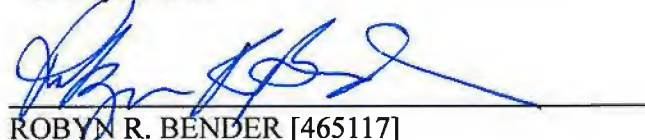
**Jury Demand**

The District of Columbia demands a trial by jury by the maximum number of jurors permitted by law.

Respectfully submitted,

Dated: December 19, 2018

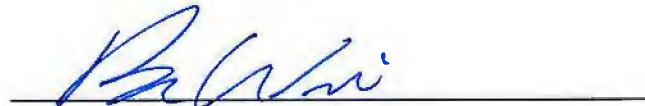
KARL A. RACINE  
Attorney General for the District of Columbia



ROBYN R. BENDER [465117]  
Deputy Attorney General  
Public Advocacy Division



JIMMY R. ROCK [493521]  
Assistant Deputy Attorney General  
Public Advocacy Division



BENJAMIN M. WISEMAN [1005442]  
Director, Office of Consumer Protection



RANDOLPH T. CHEN [1032644]  
Assistant Attorney General  
441 4th Street, N.W.  
Washington, D.C. 20001  
(202) 741-5226 (Phone)  
(202) 741-8949 (Fax)  
benjamin.wiseman@dc.gov  
randolph.chen@dc.gov

*Attorneys for the District of Columbia*